



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/568,207	06/04/2008	Christopher John Burke	SECU-PCT-US-1	8109
757 7590 05/07/2010 BRINKS HOFER GILSON & LIONE P.O. BOX 10395 CHICAGO, IL 60610				
EXAMINER RAHMAN, MOHAMMAD L				
ART UNIT 2438		PAPER NUMBER		
MAIL DATE 05/07/2010		DELIVERY MODE PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/568,207

Applicant(s)

BURKE, CHRISTOPHER JOHN

Examiner

MOHAMMAD L. RAHMAN

Art Unit

2438

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 03 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 February 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 48-64 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 48-64 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/C)
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____
- Paper No(s)/Mail Date 09/10/2009, 01/28/2010

DETAILED ACTION

This office action is issued in response to arguments/amendments filed 02/25/2010. Claims 48-64 has been amended. Claims 1-47 had previously been canceled. Claims 48-64 are still pending rejected.

Response to Arguments

Applicant's arguments/amendments, see remarks page 11-14, filed 02/25/2010 with respect to claims 49, 51, 61, and 64 have been fully considered and are persuasive to overcome rejection under 35 U.S.C. § 101. The rejections of claims 49, 51, 61, and 64 set forth in last office action under 35 U.S.C. § 101 have been withdrawn.

Independent claims 48, 49, 52, 61 have been amended to incorporate new limitation as "using a legitimate sequence of one or more biometric signals to enroll biometric signature", claims 50, 51, 62, 63, 64 have been amended to incorporate new limitation as "legitimate sequence of one or more biometric signals". Dependent claims 53-60 are also amended. Applicant's amendment to claims 48-64 filed 02/25/2010 necessitated the new ground(s) of rejection presented in this office action. Hence, Applicant's arguments/amendments filed 02/25/2010 with respect to rejection of claims 48-64 have been fully considered but are moot in view of the new ground(s) of rejection. Igaki et al. US 5,109,428 (Apr. 28, 1992) has been introduced to address the newly added limitation.

For the above reasons, it is believed that the rejections should be sustained.

Accordingly, THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 48, 49, 52, 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman et al. US 7,152,045 (hereinafter “Hoffman”) in view of Igaki et al. US 5, 109, 428 (hereinafter “Igaki”)

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Regarding claim 48, Hoffman taught a system for providing secure access to a controlled item (*see [Abstract] A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.*), the system comprising:

a transmitter subsystem (*i.e. Biometric Input Device, fig. 3 item 12*) for enrolling biometric signatures into a database (*[7:24-26] During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42, see Biometric database in fig. 2 and 44:34-36*), and for providing an accessibility attribute when

a legitimate biometric signal is received ([8:65-9:5] *The computer system would therefore maintain authenticated biometrics data samples for all authorized users of each secured computer system that it services. These data would be cross-referenced by each authorized user. Thus, after identity verification is completed, the security system provides to the user a listing of systems that he is authorized to access* see also [38:49-52] *For the CST to allow access to the database, the individual and the BIA must be identified by the system. In addition, the individual's privilege level must also be determined, so that the database can restrict access appropriately.*); and

a receiver sub-system for providing access to the controlled item dependent upon said accessibility attribute (see [Col. 40, lines 62-67] *the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute], see also [38:53-60] *An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level, Furthermore [68:10-15] *a financial transaction authorization service can decide to deny any request for over \$300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk).***

Hoffman taught the claimed system and inherently taught using a legitimate sequence of one or more biometric signals to enroll each biometric signature (Hoffman: [19:27-36] *When in scanning mode, a fingerprint scan is taken and given a preliminary analysis by the print quality*

Art Unit: 2438

algorithm. If the scan is not good enough, the BIA continues to take new scans until <time> seconds pass. As time passes and snapshots of the print are taken and analyzed....Once the print quality algorithm affirms the quality of the print scan, the print's minutiae are then extracted by the print encoding algorithm). However, the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught using a legitimate sequence of one or more biometric signals to enroll each biometric signature (see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary").

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki [Igaki:1:58-61] because the use of Igaki could provide the Biometric Input Device of Hoffman [Hoffman, fig. 3, item 12] the ability to produce a sequence of fingerprint image data from a

single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51*)).

Regarding claim 49, the combination of Hoffman and Ikagi further taught

a transmitter sub-system (Hoffman: *i.e. Biometric Input Device, fig. 3 item 12*) adapted to operate in a system configured to provide secure access to a controlled item, the system further including a processor, a memory, and a receiver sub-system configured to provide access to the controlled item dependent upon an accessibility attribute received from the transmitter sub-system (Hoffman: *see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute], see also [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.*, Furthermore [68:10-15] *a financial transaction authorization service can decide to deny any request for over \$300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.*)) ; wherein the transmitter subsystem comprises:

means for enrolling biometric signatures into the memory and a database
(Hoffman:[7:24-26] *During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal*

(BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42, see Biometric database in fig. 2 and 44:34-36), using a legitimate sequence of one or more biometric signals to enroll each biometric signature (Ikagi: see *Abstract*, “An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate.” This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad see [1:40-52] “An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary”); and

means for providing the accessibility attribute if a legitimate biometric signal is received (Hoffman: [8:65-9:5] *The computer system would therefore maintain authenticated biometrics data samples for all authorized users of each secured computer system that it services. These data would be cross-referenced by each authorized user. Thus, after identity verification is completed, the security system provides to the user a listing of systems that he is authorized to access*) see also [38:49-52] *For the CST to allow access to the database, the individual and the BIA must be identified by the system. In addition, the individual's privilege level must also be determined, so that the database can restrict access appropriately.*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki [Igaki:1:58-61] because the use of Igaki could provide the Biometric Input Device of Hoffman [Hoffman, fig. 3, item 12] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (Igaki: Col. 1:49-51).

Regarding claim 52, Hoffman taught a system for providing secure access to a controlled item (see [Abstract] *A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously.*), the system comprising:

- a database of biometric signatures [Hoffman, fig. 2, item IBD];

- a transmitter subsystem [Hoffman, fig. 3] comprising:

- a biometric sensor [Hoffman, fig.3 item 13] for receiving a biometric signal;

- means for matching the biometric signal against members of the database of biometric signatures (Hoffman: fig. 11, comparison of Biometric samples in PIC-basket with entered Bio Sample IML, see also [7:27-29] during a bid step the biometrics sample and personal identification code of the individual is gathered and compared to the ones registered during the registration step);

- means for emitting a secure access signal conveying information (Hoffman: [8:65-9:5]
The computer system would therefore maintain authenticated biometrics data samples for all authorized users of each secured computer system that it services. These data would be cross-referenced by each authorized user. Thus, after identity verification is completed, the security system provides to the user a

listing of systems that he is authorized to access) see also [38:49-52] For the CST to allow access to the database, the individual and the BIA must be identified by the system. In addition, the individual's privilege level must also be determined, so that the database can restrict access appropriately. [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level.) dependent upon said accessibility attribute; and

means for enrolling biometric signatures into the database (Hoffman, [7:24-26] During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42, see Biometric database in fig. 2 and 44:34-36, see also [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample); and

a receiver sub-system comprising;

means for receiving the transmitted secure access signal (Hoffman: fig 2, DPC is receiving biometric signal from biometric device implemented in CST/RPT/ATM); and

means for providing access to the controlled item dependent upon said information (Hoffman, see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual

is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]).

Hoffman taught the claimed system and inherently taught using a legitimate sequence of one or more biometric signals to enroll each biometric signature (Hoffman: [19:27-36] *When in scanning mode, a fingerprint scan is taken and given a preliminary analysis by the print quality algorithm. If the scan is not good enough, the BIA continues to take new scans until <time> seconds pass. As time passes and snapshots of the print are taken and analyzed....Once the print quality algorithm affirms the quality of the print scan, the print's minutiae are then extracted by the print encoding algorithm*). However, the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught using a legitimate sequence of one or more biometric signals to enroll each biometric signature (*see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate."* This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad *see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary"*).

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki [Igaki:1:58-61] because the use of Igaki could provide the Biometric Input Device of Hoffman [Hoffman, fig. 3, item 12] the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (Igaki: Col. 1:49-51).

Regarding claim 61, Hoffman taught

a transmitter subsystem [Hoffman, fig. 3] adapted to operate in a system configured to secure access to a controlled item (see [Abstract] *A tokenless identification system and method for authorization of transactions and transmissions. The tokenless system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously*), the system comprising a processor, a memory,

a database of biometric signatures [Hoffman, fig. 2, item IBD], said transmitter subsystem, and a receiver sub-system comprising

means for receiving a transmitted secure access signal (Hoffman: fig 2, DPC is receiving biometric signal from biometric device implemented in CST/RPT/ATM), and

means for providing access to the controlled item dependent upon information in said secure access signal (Hoffman, see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]), said transmitter sub-system comprising:

a biometric sensor [Hoffman, fig.3 item 13] configured to receive a biometric signal Martin, Page 4, lines 20-22];

means for emitting a secure access signal capable of granting access to the controlled item (Hoffman: [8:65-9:5] *The computer system would therefore maintain authenticated biometrics data samples for all authorized users of each secured computer system that it services. These data would be cross-referenced by each authorized user. Thus, after identity verification is completed, the security system provides to the user a listing of systems that he is authorized to access*) see also [38:49-52] *For the CST to allow access to the database, the individual and the BIA must be identified by the system. In addition, the individual's privilege level must also be determined, so that the database can restrict access appropriately. [38:53-60] *An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level*); and*

means for enrolling said biometric signatures into the memory and the database. (Hoffman, [7:24-26] *During a registration step, the individual is to register with the system an authenticated biometric sample*; [36:44-46] *The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42, see Biometric database in fig. 2 and 44:34-36, see also [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*).

Hoffman taught the claimed system and inherently taught using a legitimate sequence of one or more biometric signals to enroll each biometric signature (Hoffman: [19:27-36] *When in scanning mode, a fingerprint scan is taken and given a preliminary analysis by the print quality*

algorithm. If the scan is not good enough, the BIA continues to take new scans until <time> seconds pass. As time passes and snapshots of the print are taken and analyzed....Once the print quality algorithm affirms the quality of the print scan, the print's minutiae are then extracted by the print encoding algorithm). However, the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught using a legitimate sequence of one or more biometric signals to enroll each biometric signature (see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary").

Therefore, one of ordinary skilled artisan would have been motivated to modify the system of Hoffman with the idea of producing a sequence of fingerprint image data of Igaki [Igaki:1:58-61] because the use of Igaki could provide the Biometric Input Device of Hoffman [Hoffman, fig. 3, item 12] the ability to produce a sequence of fingerprint image data from a

single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Igaki: Col. 1:49-51*)).

Claim 62-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Igaki and in further view of Koo et al., WO 02/12660 (hereinafter "Koo")

Regarding claim 62, the combination of Hoffman and Igaki taught a transmitter sub-system according to claim 61, wherein the means for enrolling said biometric signatures into the database including sequence of legitimate biometric signal, Hoffman in view of Martin was silent on, means for storing the biometric signal received by the biometric sensor in the database as an administrator signature when the database of biometric signatures is empty; means for, when an administrator signature has been stored in the database, classifying a legitimate sequence of one or more biometric signals, each matching the administrator signature, as control information; and means for performing at least one of (a) amending information stored in the database depending upon the control information, and (b) classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information.

However Koo taught

means for storing the biometric signal received by the biometric sensor in the database as an administrator signature if the database of biometric signatures is empty (*Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14*);

means for, if an administrator signature has been stored in the database, classifying a legitimate sequence of one or more biometric signals, each matching the administrator signature,

as control information (*Koo, see the person having inputted his fingerprint is authorized as a new administrator [Page 16, lines 12-15]; and see also [Page 11, lines 16-18] the fingerprint code of the administrator is stored by receiving the code stored in the administration system*); and

means for performing at least one of (a) amending information stored in the database depending upon the control information (*Koo, see [Page 17, lines 1-5] the door lock device recognizes a new user and erases all information related to the corresponding previous card key and changes as amended the initialization completion code*), and (b) classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information (*Koo, see [Page 16, lines 10-17, the fingerprint signature is registered as administrator and see also [Page 17, lines 22-25; 18/1-3] fingerprint code is registered as the initial user fingerprint code*).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the applicant's invention was made to modify the combined method of Hoffman of Igaki with the teaching of Koo for storing biometric signal as an administrator signature and enabling administrative processing of information stored in the database if a biometric signal matching the stored administrator signature is received by the transmitter because they are analogous in biometric entry.

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo [*Page, 5, lines 19-22; Page 16, lines 8-10*] within the combined method of Hoffman [fig. 1] and Igaki because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*).

Regarding claim 63, 64, the combination of Hoffman, Igakii and Koo further taught a method of enrolling/ a computer readable storage medium having a computer program product recorded therein, [Hoffman, Col. 13, lines 51-60] when executed by a processor executes a method to enroll , by a transmitter sub-system [Hoffman, Col. 12, lines 50-55, Col. 13, lines 2-5, fig. 1 and 3], biometric signatures into a memory and a database of biometric signatures in a system for providing / configured to provide secure access to a controlled item (see [Col. 8, lines 35-40] *storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*),

the system comprising

(a) said memory and said database of biometric signatures [Hoffman, fig. 2, item IBD],

(b) the transmitter subsystem comprising a biometric sensor [Hoffman, fig.3 item 13] for receiving a biometric signal,

means for emitting a secure access signal capable of granting access to the controlled item (Hoffman: [8:65-9:5] *The computer system would therefore maintain authenticated biometrics data samples for all authorized users of each secured computer system that it services. These data would be cross-referenced by each authorized user. Thus, after identity verification is completed, the security system provides to the user a listing of systems that he is authorized to access*) see also [38:49-52] *For the CST to allow access to the database, the individual and the BIA must be identified by the system. In addition, the individual's privilege level must also be determined, so that the database can restrict access appropriately. [38:53-60] An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC privilege level) and*

means for enrolling said biometric signatures into the database (Hoffman, [7:24-26] *During a registration step, the individual is to register with the system an authenticated biometric sample; [36:44-46] The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, see further 37:12-14, 49:40-42, see Biometric database in fig. 2 and 44:34-36, see also [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample), and*

(c) a receiver sub-system comprising

means for receiving the transmitted secure access signal (Hoffman: fig 2, DPC is receiving biometric signal from biometric device implemented in CST/RPT/ATM), and

means for providing access to the controlled item dependent upon information in said secure access signal (Hoffman, see [Col. 40, lines 62-67] *the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]*), said method comprising the steps of:

receiving/code when executed by the processor, that receives a biometric signal (Hoffman: fig 2, DPC is receiving biometric signal from biometric device implemented in CST/RPT/ATM);

storing/ code when executed by the processor, that stores the biometric signal received by the biometric sensor in the database as an administrator one or more signature if the database of biometric signatures is empty (Koo, see [Page 16, lines 8-10] *if no registered administrator fingerprint*

information exists as empty, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14);

code when executed by the processor, when an administrator signature has been stored in the database, that classifies a legitimate sequence of one or more biometric signals, each signal matching the administrator signature, as control information (*Koo, see the person having inputted his fingerprint is authorized as a new administrator [Page 16, lines 12-15]; and see also [Page 11, lines 16-18] the fingerprint code of the administrator is stored by receiving the code stored in the administration system*); and

performing/ code when executed by the processor, that performs at least one of (a) amending information stored in the database depending upon the control information (*Koo, see [Page 17, lines 1-5] the door lock device recognizes a new user and erases all information related to the corresponding previous card key and changes as amended the initialization completion code*), and (b) classifying a subsequent biometric signal as one of an administrator signature and an ordinary signature depending upon the control information (*Koo, see [Page 16, lines 10-17, the fingerprint signature is registered as administrator and see also [Page 17, lines 22-25; 18/1-3] fingerprint code is registered as the initial user fingerprint code*).

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo [Page, 5, lines 19-22; Page 16, lines 8-10] within the combined method of Hoffman [fig. 1] and Igaki because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*).

Claims 50-51, 53-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffman in view of Koo and in further view of Igaki

Regarding claim 50, 51, Hoffman taught a method of by a transmitter sub-system [Hoffman, Col. 12, lines 50-55, Col. 13, lines 2-5, fig. 1 and 3], biometric signatures into a database of biometric signatures in a system for providing / a computer readable storage medium comprising a computer program recorded therein [Hoffman, Col. 13, lines 51-60] , when executed by a processor, stores in a memory and enrolls, by a transmitter subsystem, biometric signatures into a database of biometric signatures in a system configured to provide

secure access to a controlled item (Hoffman: *see [Col. 8, lines 35-40] storage of the entered biometric sample from first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample*),

the system comprising / the system comprising a processor, the memory, the transmitter sub-system and a receiver subsystem [Fig. 3] for providing / configure to provide access to the controlled item dependent upon an accessibility attribute received from the transmitter sub-system (Hoffman: *see [Col. 40, lines 62-67] the Data processing center (DPC) validates the biometric-PIC and sends the resulting asset account number along with the private code. The ATM decrypt the response, displays [Col. 41, lines 1-8] the private code and examines response to see whether or not the individual is performing a standard account access [e.g. accessibility attribute], or a "duress" account access [e.g. accessibility attribute]*);

Hoffman taught the method claim 50, 51; Hoffman was silent on, said method comprising the steps of: storing/code, when executed by the processor, that stores a biometric signal received by the transmitter sub-system in the memory and database as an administrator signature; and enabling administrative processing of information stored in the database if a biometric signal matching the stored administrator signature is received by the transmitter.

However, Koo taught

storing/code for storing a biometric signal received by the transmitter sub-system in the database as an administrator signature (*Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14*); and

enabling/code, when executed by the processor, that enables administrative processing of information stored in the database / in the memory and database when a legitimate sequences of biometric signals, each signal matching the stored administrator signature is received by the transmitter (*Koo, see [Page 5, lines 19-22] upon receiving the fingerprint information of the administrator, the door lock device unlocks the door as administrative processing, if the received fingerprint information of the administrator coincides with any one of the stored fingerprint information of the administrator*).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the applicant's invention was made to modify the method of Hoffman with the teaching of Koo for storing biometric signal as an administrator signature and enabling administrative processing of information stored in the database if a biometric signal matching the stored administrator signature is received by the transmitter because they are analogous in biometric entry. One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo [*Page, 5, lines 19-22; Page 16, lines 8-10*] within the method of Hoffman [fig. 1] because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*).

Hoffman in view of Koo taught the claimed system and inherently taught using a legitimate sequence of one or more biometric signals (Hoffman: [19:27-36] *When in scanning mode, a fingerprint scan is taken and given a preliminary analysis by the print quality algorithm. If the scan is not good enough, the BIA continues to take new scans until <time> seconds pass. As time passes and snapshots of the print are taken and analyzed....Once the print quality algorithm affirms the quality of the print scan, the print's minutiae are then extracted by the print encoding algorithm*). However, the analogous art Igaki which addressed the same field of endeavor in fingerprint identification explicitly taught using a legitimate sequence of one or more biometric signals to enroll each biometric signature (see Abstract, "An optical sensor unit optically produces a sequence of fingerprint image data during a single operation of pressing a fingerpad onto an inspection plate in a direction substantially transverse to the plate and with increasing pressure over a time interval. A data storing unit stores the produced fingerprint image data in the form of a sequence of fingerprint image data obtained during the single operation of pressing the fingerpad onto the inspection plate." This method is the improvement from already known successive multiple fingerprint pressing down operations to performing only a single operation of pressing down of the fingerpad see [1:40-52] "An object of the present invention is to provide an improved apparatus and method for use in fingerprint identification for extracting minutia data from fingerprint image data in which a plurality of picking-up operations of the fingerprint image data is carried out by performing only a single operation of pressing down of the fingerpad, on a sensor the alignment between successive fingerprint image data produced in successive, multiple fingerprint pressing down operations as in the prior art becomes unnecessary").

Therefore, one of ordinary skilled artisan would have been motivated to modify the combined system of Hoffman and Koo with the idea of producing a sequence of fingerprint image data of Igaki [Igaki:1:58-61] because the use of Igaki could provide the combined system

of Biometric Input Device of Hoffman [*Hoffman, fig. 3, item 12*] and Koo the ability to produce a sequence of fingerprint image data from a single operation of pressing down of the fingerpad so that the troublesome process of the repeated fingerpad pressing down operation is eliminated (*Ikagi: Col. 1:49-51*).

Regarding claim 53, the combination of Hoffman, Koo, and Igaki further taught a system according to claim 52, wherein the means for enrolling biometric signatures comprises:

means for determining when the database of biometric signatures is empty (*Koo, see [Page, 16, lines 5-9] the controller search the registered administrator fingerprint code information to see if there is no administrator fingerprint information exists as empty*); and

means for storing a biometric signal received by the biometric sensor in the database as an administrator signature when the database of biometric signatures is empty (*Koo, see [Page 16, lines 8-10] if no registered administrator fingerprint information exists, the inputted fingerprint is registered as initial administrator fingerprint, see also page 10, lines 12-14*).

One of ordinary skilled in the art would have been motivated to incorporate the idea of Koo [*Page, 5, lines 19-22; Page 16, lines 8-10*] within the method of Hoffman [*fig. 1*] because the idea of Koo could provide the method of Hoffman to provide an electronic card key administration system consisted of host computer systems for administration of a plural of the electronic fingerprint recognition card keys (*Koo, Page 3, lines 21-23*)

Regarding claim 54, the combination of Hoffman, Koo, and Igaki further taught a system according to claim 53, wherein the means for enrolling biometric signatures further comprises means for, when an administrator signature has been stored in the database, classifying the legitimate sequence of biometric signals, each signal matching the administrator

signature, as control information (*Koo, see the person having inputted his fingerprint is authorized as a new administrator [Page 16, lines 12-15]; and see also [Page 11, lines 16-18] the fingerprint code of the administrator is stored by receiving the code stored in the administration system*).

Regarding claim 55, the combination of Hoffman, Koo, and Igaki further taught a system according to claim 54, wherein the means for enrolling biometric signatures further comprises means for determining when said sequence of biometric signals is legitimate dependent upon whether at least one of the number and duration of the signals are appropriate, and whether the signals are received within a predetermined time (*Hoffman, see [Col. 19, lines 16-35] the BIA continues to take new scans until <time> seconds pass. As time passes and snapshots of the print are taken and analyzed, if no print of appropriate quality is forthcoming, the BIA returns an error code of time expired. See also [Col. 19, lines 64-65], scanning terminates when either <time> number of seconds runs out, when the individual hits the "enter" key*).

Regarding claim 56, the combination of Hoffman, Koo, and Igaki further taught a system according to claim 54, wherein the means for enrolling biometric signatures further comprises means for amending information stored in the database depending upon the control information (*Koo, see [Page 17, lines 1-5] the door lock device recognizes a new user and erases all information related to the corresponding previous card key and changes as amended the initialization completion code*).

Regarding claim 57, the combination of Hoffman and Koo further taught a system according to claim 54, wherein the means for enrolling biometric signatures further comprises means for classifying a subsequent biometric signal as one of an administrator signature and an

ordinary signature depending upon the control information (*Koo, see [Page 16, lines 10-17, the fingerprint signature is registered as administrator and see also [Page 17, lines 22-25; 18/1-3] fingerprint code is registered as the initial user fingerprint code).*

Regarding claim 58, Hoffman in view of Igaki further taught a system according to claim 48, wherein the transmitter sub-system is incorporated into at least one of (a) a remote control module comprising at least one of a key fob and a mobile communication device, and (b) an enclosure mounted next to the controlled item [*Hoffman, fig. 1, CATV, PPT, and fig. 2*].

Regarding claim 59, Hoffman, in view of Koo, and Igaki further taught a system according to claim 53 further comprising means for providing a feedback signal for directing input of the control information (*Hoffman, see [Col. 19, lines 34-35, 42-43] the BIA returns an error code and display a message if fingerprint quality is not good or legitimate and responds with the success result code if print quality algorithm affirm the quality of scan).*

Regarding claim 60, Hoffman in view of Koo and Igaki further taught a system according to claim 59, wherein the means for providing the feedback signal comprises at least one of a visual indicator and an audio indicator (*Hoffman, see [Col. 19, lines 35-36; fig. 3] the BIA display response on the LCD).*

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. Hayakawa et al. US 2002/0130764 id cited for the teaching of **Biometric information registration** and authentication [fig.1, 4].

2. Voltmer et al. US 2002/0112177 is cited for the teaching of setting of privileges based on biometric sample (fig. 12A).

Applicant's amendment to claims 48-64 necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MOHAMMAD L. RAHMAN whose telephone number is (571)270-7471. The examiner can normally be reached on Monday-Friday (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T. Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 10/568,207
Art Unit: 2438

Page 26

/M. L. R./
Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438